No. 90-1876

FILED
JUN 5 1991
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

October Term 1990

ROBERT TAPPAN MORRIS

Petitioner,

v.

UNITED STATES OF AMERICA

Respondent.

PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

THOMAS A. GUIDOBONI
BONNER & O'CONNELL
Suite 1000
900 Seventeenth Street, NW
Washington, D.C. 20006
(202) 452-1300

Counsel of Record for Petitioner

CASILLAS PRESS, INC., 1717 K STREET, N.W., WASHINGTON, D.C. 20036

QUESTION PRESENTED FOR REVIEW

Does 18 U.S.C. § 1030(a)(5)(A) permit conviction in the absence of proof that a defendant intended to cause the resulting injury?

TABLE OF CONTENTS

Page

QUESTION PRESENTED FOR REVIEW i

TABLE OF AUTHORITIES v

OPINIONS BELOW 1

JURISDICTION 2

STATUTES INVOLVED 2

STATEMENT OF THE CASE 2

REASONS FOR GRANTING THE WRIT 8

CONCLUSION 12

APPENDIX A

Opinion of the United States Court of Appeals for the Second Circuit (March 7, 1991) 1a

APPENDIX B

Opinions and Orders of the United States District Court for the Northern District of New York 20a

Judgment Including Sentence (May 16, 1990) 20a

Oral Decision Denying Post-Trial Motions (February 27, 1990) 27a

Oral Decision Denying Motion for Judgment of Acquittal (January 18, 1990) 35a

Page

Oral Decision Denying Motion for Judgment of Acquittal (January 17, 1990).....37a

Memorandum-Decision & Order Permitting The United States to Withdraw a Portion of the Indictment (January 3, 1990).....39a

Oral Decisions Denying Motions to Dismiss the Indictment (November 3, 1989).....43a

APPENDIX C

Text of Statutes Involved

18 U.S.C. § 1030 (1988).....52a
18 U.S.C. § 1030 (Supp. II, 1984).....58a

TABLE OF AUTHORITIES

Cases: Page

Liparota v. United States,
471 U.S. 419 (1985).....9

Morisette v. United States,
342 U.S. 246 (1952).....8

Taylor v. United States,
110 S. Ct. 2143 (1990).....11

United States v. Bailey,
444 U.S. 394 (1980).....10

United States v. Bass
404 U.S. 336 (1971).....12

United States v. Johnson & Towers, Inc.,
741 F.2d 662 (3rd Cir. 1984), *cert. denied*,
469 U.S. 1208 (1985).....9

United States v. Marvin, 687 F.2d 1221 (8th
Cir. 1982), *cert. denied*, 460 U.S. 1081 (1983).....9

United States v. Nofziger, 878 F.2d 442
(D.C. Cir.), *cert. denied*, 110 S.Ct.
564 (1989).....9

United States v. O'Brien, 686 F.2d 850
(10th Cir. 1982).....9

United States v. United States Gypsum Co.,
438 U.S. 422 (1978).....8,11

United States v. Yermian,
469 U.S. 63 (1984).....9

Page

STATUTES:

18 U.S.C. § 1030 (1988).....2

18 U.S.C. § 1030 (a)(5)(A) (1988).....i, 3, 6, 7, 8, 10

18 U.S.C. § 1030 (Supp. II, 1984).....2

18 U.S.C. § 1030(a)(3) (Supp. II, 1984).....10, 11

18 U.S.C. § 3231.....3

28 U.S.C. § 1254(1).....2

Computer Fraud and Abuse Act of 1986
Pub. L. No. 99-474, 100 Stat. 1213 (1986).....3, 6

OTHER AUTHORITIES:

132 Cong. Rec. H3275 (daily ed. June 3, 1986).....10

S. Rep. No. 432 (Judiciary Committee), 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 2479.....10, 11

H.R. Rep. No. 612 (Judiciary Committee), 99th Cong., 2d Sess (1986).....9, 10

General Accounting Office, Rept. to the Chairman, Subcomm. on Telecommunications and Finance, Comm. on Energy and Commerce, H.R., *Computer Security Virus Highlights Need for Improved Internet Management* (June 1989).....11, 12

Tompkins & Ansell, *Computer Crime: Keeping Up With High Tech Crimes*, CRIM. JUST. 30 (Winter 1987).....11

IN THE

Supreme Court of the United States

October Term 1990

No.

ROBERT TAPPAN MORRIS

Petitioner,

v.

UNITED STATES OF AMERICA

Respondent.

PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

The Petitioner, ROBERT TAPPAN MORRIS, respectfully prays that a Writ of Certiorari be issued to review the judgment and opinion of the United States Court of Appeals for the Second Circuit, entered on March 7, 1991.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Second Circuit is reported at 928 F.2d 504 (2d Cir. 1991), and is printed as Appendix A. The judgment (Including Sentence) of the United States District Court for the Northern District of New York, entered May 16, 1990, is unreported and is printed in Appendix B at p. 20a. The orders and opinions of the United States District Court for the Northern

District of New York which: (1) denied Petitioner's motions for judgment of acquittal and alternatively for a new trial on February 27, 1990; (2) denied Petitioner's motions for judgment of acquittal on January 17 and 18, 1990; and (3) denied Petitioner's motions to dismiss the indictment on November 3, 1989; are unreported, and are printed in Appendix B at pages 27a, 35a, 37a, and 43a, respectively.

The memorandum decision and order granting the motion of the United States to withdraw a portion of the indictment, entered January 3, 1990, is reported at 728 F. Supp. 85 (N.D.N.Y. 1990), and is printed in Appendix B at p. 39a.

JURISDICTION

The judgment of the United States Court of Appeals for the Second Circuit affirming Petitioner's conviction was entered on March 7, 1991. No petition for rehearing was sought. The jurisdiction of this Court to review the judgment of the Second Circuit is invoked under 28 U.S.C. § 1254(1).

STATUTES INVOLVED

The text of 18 U.S.C. § 1030 (1988) is printed in Appendix C at p. 52a. Also involved in the case is the prior version of the same statute, 18 U.S.C. § 1030 (Supp. II, 1984), which is printed in Appendix C at p. 58a.

STATEMENT OF THE CASE

The petition seeks review of the judgment of the United States Court of Appeals for the Second Circuit affirming the conviction of Petitioner Robert Tappan Morris by the United States District Court for the Northern District of New York in connection with his creation and release of a computer pro-

gram known as a "virus" or "worm"[1] into the INTERNET, a national computer network linking various educational institutions, research centers, and military facilities. This program, once released, spread and multiplied causing some of the computers at these various sites to "crash" or cease functioning.

Mr. Morris was charged with violating the Computer Fraud and Abuse Act of 1986,[2] 18 U.S.C. § 1030(a)(5)(A), in the first reported prosecution under the statute. The District Court's jurisdiction was based on 18 U.S.C. § 3231.

FACTS

In the fall of 1988, Robert Tappan Morris was a 22 year old first year student, enrolled as a Ph.D. candidate in computer science at Cornell University. Through his undergraduate studies at Harvard, and various jobs he had held, Petitioner acquired a high degree of computer experience and expertise. He published several technical papers, and had lectured on computer security at the National Computer Security Center of the National Security Agency, and the United States Naval Research Laboratory.

When Petitioner enrolled at Cornell, he was given an account on the computers at the Computer Science Department, by virtue of which he was explicitly authorized to use the computers at Cornell. Morris openly discussed with fellow graduate students, including the son of the Chairman of the Department of Computer Science at Cornell, the level of security

---

[1]A "worm" is a computer program which travels from one computer to another but does not attach itself to the operating systems of the computers. A "virus" is also a migratory program, but it attaches itself to the operating program of any computer it enters. Morris' creation is properly referred to as a "worm". See United States v. Morris, 928 F.2d 504, 505 & n.1 (2d Cir. 1991).

[2]Pub. L. No. 99-474, 100 Stat. 1213 (1986)

on computer networks, and his ability to by-pass it.

In mid -October, 1988, Petitioner began work on the computer program which later became known as the INTERNET "worm". He saw this work as an experimental attempt to write a program which would spread as widely as possible to certain types of computers connected to the INTERNET by exploiting security defects. Petitioner's goal was to have this worm spread widely without attracting attention to itself. Thus, it was designed to use little computer operation time or resources, so that it would not interfere with the normal work of the computers. Morris also thought "it would be bad if the program somehow made it harder for other people to use the [computer] systems the worm was running on" (Tr. 1090)[3]

Petitioner also programmed the worm to be difficult to detect and to read so that others could not easily defend against it, because a worm which was easily "killed" was not likely to spread very far. Finally, according to a friend with whom he shared hs concept, Petitioner "specifically intended not to destroy data or cause people trouble" by reading their data files or causing their computers to cease functioning (Tr. 983-84).

To some extent these multiple goals were in conflict. One of the most difficult problems for Petitioner was how to limit the growth, or number of copies of the worm program on any particular computer. Multiple copies would not only make the worm highly visible, but also would overload the system and ultimately cause the computer to cease functioning. After discarding several concepts, Morris concluded that he would structure the worm program so that each newly arriving worm would "ask" the computer if any copies of itself were already present. If the computer responded "no", then the worm

[3] "Tr." references are to the transcript of trial testimony.

would copy itself onto the computer. If it responded "yes", then the worm would not duplicate itself onto that machine.

This solution raised another difficulty, however. Other programmers could easily defeat the worm by programming their machines to answer the worm's inquiry with a false "yes", thereby turning away the worm, and limiting its spread. To avoid this potential defense mechanism, Morris designed the worm to duplicate itself every seventh time that it received a positive answer. This repetition was intended to insure the worm's survival. The worm program was also written so that it would be killed off whenever a computer was shut down, an event which typically occurs for repairs or administrative reasons about once a week. Had Petitioner correctly estimated the likely rate of reinfection, ordinary procedures would have removed the worm program from any computer system within a week or two.

As it turned out, Morris underestimated the number of times a computer was queried by a new worm program seeking to gain entry, and the one to seven ratio permitted far more copying of the program than Morris had foreseen. The government's expert witness acknowledged that this portion of the worm program was an attempt to limit the growth of the worm on any particular computer, and conceded that there would be no reason to include such a limitation if the worm's creator had wanted the worm to reproduce rapidly (Tr. 448-49).

At about 8:00 p.m. on Novermber 2, 1988, Petitioner released the worm onto the INTERNET by electronically transferring the program from a computer at Cornell to a computer at the Massachusetts Institute of Technology. Once the program was launched, Petitioner had no ability to control it, and only limited opportunity to observe it. Later that evening he discovered that the worm was replicating much faster than he had anticipated, thereby multiplying on many individual

machines and slowing them down dramatically. He contacted some friends at Harvard to discuss possible solutions. They sent out an anonymous message from Havard over the network, which contained an apology and instructions to programmers at other facilities on how to kill the worm and prevent further reinfection. Unfortunately, because the electronic route was clogged, the message was not received until it was too late to do any good.

The worm spread rapidly over the INTERNET, and by the next day had slowed down or stopped computers at numerous universities, and other research facilities. Although the worm caused no permanent damage or destruction, the estimated costs of combatting it ranged from a low of $200 to a high of $53,00 at the various facilities. On November 3, 1988, Morris telephoned his father, who was the chief scientist at the National Computer Security Center of the National Security Agency of the United States, and admitted his responsibility for creating the worm program.

Legal Proceedings

On July 26, 1989, a federal grand jury, sitting in the Northern District of New York, returned a single count indictment charging Petitioner with a violation of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5)(A). Morris entered a plea of not guilty and demanded trial by jury. Prior to trial, Petitioner filed two separate motions to dismiss the indictment. One of these motions challenged the sufficiency of the indictment for failing to allege all the essential elements of the offense, in particular, the element of intent. The District Court denied Petitioner's motions in an oral opinion rendered on November 3, 1989, *see* Appendix B at p. 43a. Thereafter, the government sought to withdraw a portion of the indictment, and over Morris' opposition, this motion was granted

by written decision and Order dated January 3, 1990. 728 F. Supp. 95; Appendix B at p. 39a.

Trial with a jury commenced on January 8, 1991. Petitioner's motion for judgment of acquittal at the close of the government's case in chief was denied by oral order on January 17, 1990. See Appendix B at p. 37a. His motion for judgment of acquittal at the conclusion of all the evidence was likewise denied on January 18, 1990. *See* Appendix B at p. 35a. Both of these motions were grounded in part upon the government's failure to prove the requisite intent. Petitioner's proposed jury instructions on the intent element were subsequently rejected, and the jury returned a verdict of guilty on January 22, 1990.

Petitioner's post-trial motions for judgment of acquittal or alternatively, for a new trial, were denied by oral opinion on February 27, 1990, *see,* Appendix B at p. 27a. These motions also were based, *inter alia,* on the intent element of the offense. On May 4, 1990, Morris was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision. The written judgment and sentence was filed on May 16, 1990. Appendix B at p. 20a.

A timely appeal was taken to the United States Court of Appeals for the Second Circuit. In its opinion, reported at 928 F.2d 504, the Second Circuit held that 18 U.S.C. § 1030(a)(5)(A) did not require the government to prove that Petitioner had intentionally prevented authorized use of a federal interest computer and thereby caused loss (*See* Appendix A at p. 3a). It also held the evidence sufficient for the jury to conclude that Petitioner acted "without authorization" (*Id.*)[4] Accordingly, the judgment of conviction was affirmed, Appendix A at p. 19a.

[4]Petitioner does not seek review of this second holding.

REASONS FOR GRANTING THE WRIT

1. The decision of the Second Circuit has excised from a federal criminal statute compliance with the universal and persistent tenet "that an injury can amount to a crime only when inflected by intention. . . ." *Morissette v. United States*, 342 U.S. 246, 250 (1952). In so doing, the Court of Appeals ignored the intent of Congress, and decisions of other federal courts in similar cases. Moreover, its decision to eliminate the requirement of proof of an intent to cause injury, directly contradicts this Court's decision in *United States v. United States Gypsum Co.*, 438 U.S. 422 (1978) which holds that "far more than the simple omission of the appropriate phrase from the statutory definition is necessary to justify dispensing with an intent requirement." 438 U.S. at 438.

2. The statute under which Petitioner was convicted punishes as a felon, anyone who:

> *intentionally accesses* a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or *prevents authorized use* of any such computer or information, and *thereby*
>
> (1) *causes loss* to one or more others of a value aggregating $1,000 or more during any one year period. . . .

18 U.S.C. § 1030(a)(5)(A) (emphasis added).[5] The government maintained, and the Second Circuit accepted, ". . . that the 'intentionally' standard applies only to the 'access' phrase of § 1030(a)(5)(A), and not to its 'damages' phrase." 928 F.2d

[5]Morris was charged only under the "prevents authorized use" portion of the statute.

at 509; Appendix A at p. 13a. This ruling, which rendered irrelevant Petitioner's lack of intent to cause harm, is at odds with this Court's decision in *Liparota v. United States*, 471 U.S. 419 (1985) (interpreting food stamps statute), as well as decisions by the United States Courts of Appeals for the District of Columbia Circuit in *United States v. Nofziger*, 878 F.2d 442 (D.C. Cir.) (interpreting conflict of interest statute), *cert. denied*, 110 S.Ct. 564 (1989), and the Third Circuit in *United States v, Johnson & Towers, Inc.*, 741 F.2d 662 (3d Cir. 1984) (interpreting hazardous waste law), *cert. denied*, 469 U.S. 1208 (1985). In each of these cases the Court ruled that the explicit state of mind requirement extended to modify a string of clauses containing additional elements of the offense.[6] In the instant case, where the statute is similarly structured, and the additional elements relate directly to resulting harm, the Second Circuit has reached a contrary and unwarranted result.[7]

3. The Circuit Court's conclusion appears contrary as well to the weight of the legislative history. The Judiciary Committees of both Houses of Congress articulated their choice of the "intentional" state of mind as based on the understanding that:

> . . . a person who causes a particular result is said to act purposely (intentionally) when he consciously desires that result, whatever the likelihood of that result happening from his conduct. . .

H.R. Rep. No. 612 (Judiciary Committee) 99th Cong., 2d Sess.

---

[6]The Eighth and Tenth Circuits reached the same conclusion interpreting the statute before this Court in *Liparota. United States v. Marvin*, 687 F.2d 1221 (8th Cir. 1982), *cert. denied*, 460 U.S. 1081 (1983); *Untied States v. O'Brien*, 686 F.2d 850 (10th Cir. 1982).

[7]This case is distinguishable from *United States v. Yermian*, 468 U.S. 63 (1984), where this Court held in a 5 to 4 decision that the state of mind requirement did not modify the jurisdictional language.

at 9-10 (1986), quoting *United States v. Bailey*, 444 U.S. 394 (1980); *See* S. Rep. No. 432 (Judiciary Committee), 99th Cong. 2d. Sess. at 5-6 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 2479, 2483-84. The Senate Report goes on to describe the law as one ". . . designed to penalize those who *intentionally alter, damage* or *destroy* certain computerized data." S. Rep. No. 432, *supra* at 10, U.S. Code Cong. & Admin. News at 2488 (emphasis added). The House Report describes the offense as a "*malacious damage felony* violation." H.R. Rep. No. 612, *supra* at 12 (emphasis added). Similar language was utilized by members of the Judiciary Committee during the floor debates, 132 Cong. Rec. H3275, H3276 (daily ed. June 3, 1986) (remarks of Rep. Hughes); *Id.* at H3278 (remarks of Chairman Rodino).

4. Characterizing this consistent history as mere "isolated language," 928 F.2d at 509; Appendix A at p. 13a, the Second Circuit chose instead to rely on a comparison between the format of the current version of § 1030(a)(5) with that of its predecessor, § 1030(a)(3) (Supp. II, 1984); Appendix C at p. 58a. The 1984 version covered anyone who:

> *knowingly* accesses a computer without authorization, *or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend*, and by means of such conduct *knowingly* uses, modifies, destroys, or discloses information in, or prevents authorized use of such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;

(emphasis added). The Second Circuit reasoned that because Congress omitted repetition of the state of mind requirement in the 1986 version, it did not intend to extend the state of

mind element beyond the "access" phrase of the statute. 928 F.2d at 509, Appendix A at p. 13a.

In this case, however, like *Taylor v. United States*, 110 S. Ct. 2143 (1990), nothing in the legislative history demonstrates that Congress intended to abandon its previous approach [110 S. Ct. 2153-54]. Indeed, it is more likely that Congress struck the additional "knowingly" from the statute because it had also deleted that portion of the offense applying to a person who:

> . . . having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend. . . .

18 U S.C. § 1030(a)(3) (Supp. II, 1984). Deletion from the offense of this "cumbersome phrase," S. Rep. No. 432, *supra* at 9, U.S. Code Cong. & Admin. News at 2486, and limitation of the scope of the prohibition to ". . . those lacking authorization to access any Federal interest computer," S. Rep. No. 432, *supra* at 10, U.S. Code Cong. & Admin. News at 2488, rendered the second "knowingly" redundant. In any event, its mere omission from the 1986 version does not support the Second Circuit's conclusion that proof of an intention to cause injury is not required. *See United States v. United States Gypsum Co.*, *supra* 438 U.S. at 438.

Elimination of the "intent to cause injury" element is particularly troublesome where the offense involves a new, complex, and evolving technology, and the statutory language has been criticized as lacking clarity and definition of its elements. *See* Tompkins & Ansell, *Computer Crime: Keeping Up With High Tech Crimes*, CRIM. JUST. 30, 44 (Winter 1987); General Accounting Office, Rept. to the Chairman, Subcomm. on Telecommunications and Finance, Comm. on Energy and

Commerce, H.R., *Computer Security Virus Highlights Need for Improved Internet Management* at 31 (June 1989). Under these circumstances, a decision which permits conviction of an individual lacking the purpose to cause harm, violates the traditional rule that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *United States v. Bass*, 404 U.S. 336, 347 (1971).

The Second Circuit's decision will also stifle the creativity of those computer scientists whose experiments have been responsible for many advances in this critical field of endeavor. This Court can correct these unwarranted consequences by granting plenary review.

CONCLUSION

For these reasons, a Writ of Certiorari should be granted to review the judgment of the United States Court of Appeals for the Second Circuit.

Respectfully submitted,
BONNER & O'CONNELL

By _____
Thomas A. Guidoboni
Suite 1000
900 Seventeenth Street, N.W.
Washington, D.C. 20006
(202) 452-1300
Counsel of Record for Robert Tappan Morris, Petitioner

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

No. 774—August Term, 1990

Argued: December 4, 1990 — Decided: March 7, 1991

Docket No. 90-1339

UNITED STATES OF AMERICA,

Appellee,

—v.—

ROBERT TAPPAN MORRIS,

Defendant-Appellant.

Before:

NEWMAN and WINTER, *Circuit Judges*,
and DAVIS,* *District Judge*.

Appeal from the May 16, 1990, judgment of the District Court for the Northern District of New York (Howard G. Munson, Judge) convicting defendant on one count of violating the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5) (1988).

Affirmed.

---

* The Honorable T.F. Gilroy Daly of the District Court for the District of Connecticut, sitting by designation.

APPENDIX A

UNITED STATES COURT OF APPEALS

FOR THE SECOND CIRCUIT

No. 774—August Term 1990

Argued: December 4, 1990 Decided: March 7, 1991

Docket No. 90-1336

UNITED STATES OF AMERICA,

Appellee,

—v.—

ROBERT TAPPAN MORRIS,

Defendant-Appellant.

Before:

NEWMAN and WINTER, *Circuit Judges*,
and DALY, *District Judge*.*

Appeal from the May 16, 1990, judgment of the District Court for the Northern District of New York (Howard G. Munson, Judge) convicting defendant on one count of violating the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5) (1988).

Affirmed.

* The Honorable T.F. Gilroy Daly of the District Court for the District of Connecticut, sitting by designation.

THOMAS A. GUIDOBONI, Wash., D.C., *for defendant-appellant*.

ELLEN R. MELTZER, U.S. Dept. of Justice, Wash., D.C. (Frederick J. Scullin, Jr., U.S. Atty., Syracuse, N.Y.; Mark D. Rasch, U.S. Dept. of Justice, Wash., D.C., on the brief), *for appellee*.

JON O. NEWMAN, *Circuit Judge*:

This appeal presents two narrow issues of statutory construction concerning a provision Congress recently adopted to strengthen protection against computer crimes. Section 2(d) of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5)(A) (1988), punishes anyone who intentionally accesses without authorization a category of computers known as "[f]ederal interest computers" and damages or prevents authorized use of information in such computers, causing loss of $1,000 or more. The issues raised are (1) whether the Government must prove not only that the defendant intended to access a federal interest computer, but also that the defendant intended to prevent authorized use of the computer's information and thereby cause loss; and (2) what satisfies the statutory requirement of "access without authorization?"

These questions are raised on an appeal by Robert Tappan Morris from the May 16, 1990, judgment of the District Court for the Northern District of New York (Howard G. Munson, Judge) convicting him, after a jury trial, of violating 18 U.S.C. § 1030(a)(5)(A). Morris released into INTERNET, a national computer network,

a computer program known as a "worm"[1] that spread and multiplied, eventually causing computers at various educational institutions and military sites to "crash" or cease functioning.

We conclude that subsection 1030(a)(5)(A) does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss. We also find that there was sufficient evidence for the jury to conclude that Morris acted "without authorization" within the meaning of subsection 1030(a)(5)(A). We therefore affirm.

Facts

In the fall of 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

In October 1988, Morris began work on a computer program, later known as the INTERNET "worm" or "virus." The goal of this program was to demonstrate

---

1 In the colorful argot of computers, a "worm" is a program that travels from one computer to another but does not attach itself to the operating system of the computer it "infects." It differs from a "virus," which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer.

the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. The tactic he selected was release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into INTERNET, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network.

Morris sought to program the INTERNET worm to spread widely without drawing attention to itself. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily.

Morris also wanted to ensure that the worm did not copy itself onto a computer that already had a copy. Multiple copies of the worm on a computer would make the worm easier to detect and would bog down the system and ultimately cause the computer to crash. Therefore, Morris designed the worm to "ask" each computer whether it already had a copy of the worm. If it responded "no," then the worm would copy onto the computer; if it responded "yes," the worm would not duplicate. However, Morris was concerned that other programmers could kill the worm by programming their own computers to falsely respond "yes" to the question. To circumvent this protection, Morris programmed the worm to duplicate itself every seventh time it received a

"yes" response. As it turned out, Morris underestimated the number of times a computer would be asked the question, and his one-out-of-seven ratio resulted in far more copying than he had anticipated. The worm was also designed so that it would be killed when a computer was shut down, an event that typically occurs once every week or two. This would prevent the worm from accumulating on one computer, had Morris correctly estimated the likely rate of reinfection.

Morris identified four ways in which the worm could break into computers on the network:

> (1) through a "hole" or "bug" (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer;
>
> (2) through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer;
>
> (3) through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and
>
> (4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discov-

ered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

Morris was found guilty, following a jury trial, of violating 18 U.S.C. § 1030(a)(5)(A). He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.

Discussion

I. The intent requirement in subsection 1030(a)(5)(A)

Subsection 1030(a)(5)(A), covers anyone who

> (5) *intentionally accesses* a Federal interest computer without authorization, *and* by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or *prevents authorized use* of any such computer or information, *and thereby*
>
> (A) *causes loss* to one or more others of a value aggregating $1,000 or more during any one year period; . . . [emphasis added].

The District Court concluded that the intent requirement applied only to the accessing and not to the resulting damage. Judge Munson found recourse to legislative history unnecessary because he considered the statute clear and unambiguous. However, the Court observed that the legislative history supported its reading of subsection 1030(a)(5)(A).

Morris argues that the Government had to prove not only that he intended the unauthorized access of a federal interest computer, but also that he intended to prevent others from using it, and thus cause a loss. The adverb "intentionally," he contends, modifies both verb phrases of the subsection. The Government urges that since punctuation sets the "accesses" phrase off from the subsequent "damages" phrase, the provision unambiguously shows that "intentionally" modifies only "accesses." Absent textual ambiguity, the Government asserts that recourse to legislative history is not appropriate. *See Burlington N.R. Co. v. Oklahoma Tax Comm'n*, 481 U.S. 454, 461 (1987); *Consumer Product Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980); *United States v. Holroyd*, 732 F.2d 1122, 1125 (2d Cir. 1984).

With some statutes, punctuation has been relied upon to indicate that a phrase set off by commas is independent of the language that followed. *See United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989) (interpreting the Bankruptcy Code). However, we have been advised that punctuation is not necessarily decisive in construing statutes, *see Costanzo v. Tillinghast*, 287 U.S. 341, 344 (1932), and with many statutes, a mental state adverb adjacent to initial words has been applied to phrases or clauses appearing later in the statute with-

out regard to the punctuation or structure of the statute. *See Liparota v. United States*, 471 U.S. 419, 426-29 (1985) (interpreting food stamps provision); *United States v. Nofziger*, 878 F.2d 442, 446-50 (D.C. Cir.) (interpreting government "revolving door" statute), *cert. denied*, 110 S. Ct. 564 (1989); *United States v. Johnson & Towers, Inc.*, 741 F.2d 662, 667-69 (3d Cir. 1984) (interpreting the conservation act), *cert. denied*, 469 U.S. 1208 (1985). In the present case, we do not believe the comma after "authorization" renders the text so clear as to preclude review of the legislative history.

The first federal statute dealing with computer crimes was passed in 1984, Pub. L. No. 98-473, (codified at 18 U.S.C. § 1030 (Supp. II 1984)). The specific provision under which Morris was convicted was added in 1986, Pub. L. No. 99-474, along with some other changes. The 1986 amendments made several changes relevant to our analysis.

First, the 1986 amendments changed the scienter requirement in subsection 1030(a)(2) from "knowingly" to "intentionally." *See* Pub. L. No. 99-474, section 2(a)(1). The subsection now covers anyone who

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

According to the Senate Judiciary Committee, Congress changed the mental state requirement in subsection 1030(a)(2) for two reasons. Congress sought only to proscribe intentional acts of unauthorized access, not "mistaken, inadvertent, or careless" acts of unauthorized access. S. Rep. No. 99-432, 99th Cong., 2d Sess. 5 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 2479, 2483 [hereinafter Senate Report].

Also, Congress expressed concern that the "knowingly" standard "might be inappropriate for cases involving computer technology." *Id.* The concern was that a scienter requirement of "knowingly" might encompass the acts of an individual "who inadvertently 'stumble[d] into' someone else's computer file or computer data," especially where such individual was authorized to use a particular computer. *Id.* at 6, 1986 U.S. Code Cong. & Admin. News at 2483. The Senate Report concluded that "[t]he substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." *Id.*, U.S. Code Cong. & Admin. News at 2484. Congress retained the "knowingly" standard in other subsections of section 1030. *See* 18 U.S.C. § 1030(a)(1), (a)(4).

This use of a *mens rea* standard to make sure that inadvertent accessing was not covered is also emphasized in the Senate Report's discussion of subsection 1030(a)(3) and subsection 1030(a)(5), under which Morris was convicted. Both subsections were designed to target "outsiders," individuals without authorization to access any federal interest computer. Senate Report at 10, U.S. Code Cong. & Admin. News at 2488. The

rationale for the *mens rea* requirement suggests that it modifies only the "accesses" phrase, which was the focus of Congress's concern in strengthening the scienter requirement.

The other relevant change in the 1986 amendments was the introduction of subsection (a)(5) to replace its earlier version, subsection (a)(3) of the 1984 act, 18 U.S.C. § 1030(a)(3) (Supp. II 1984). The predecessor subsection covered anyone who

> knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of United States and such conduct affects such operation.

The 1986 version changed the mental state requirement from "knowingly" to "intentionally," and did not repeat it after the "accesses" phrase, as had the 1984 version. By contrast, other subsections of section 1030 have retained "dual intent" language, placing the scienter requirement at the beginning of both the "accesses" phrase and the "damages" phrase. *See, e.g.*, 18 U.S.C. § 1030(a)(1).

Morris notes the careful attention that Congress gave to selecting the scienter requirement for current subsections (a)(2) and (a)(5). Then, relying primarily on comments in the Senate and House reports, Morris argues that the "intentionally" requirement of subsec-

tion 1030(a)(5)(A) describes both the conduct of accessing and damaging. As he notes, the Senate Report said that "[t]he new subsection 1030(a)(5) to be created by the bill is designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another." Senate Report at 10, U.S. Code Cong. & Admin. News at 2488. The House Judiciary Committee stated that "the bill proposes a new section (18 U.S.C. 1030(a)(5)) which can be characterized as a 'malicious damage' felony violation involving a Federal interest computer. We have included an 'intentional' standard for this felony and coverage is extended only to outside trespassers with a $1,000 threshold damage level." H.R. Rep. No. 99-612, 99th Cong. 2d Sess. at 7 (1986). A member of the Judiciary Committee also referred to the subsection 1030(a)(5) offense as a "malicious damage" felony during the floor debate. 132 Cong. Rec. H3275, 3276 (daily ed. June 3, 1986) (remarks of Rep. Hughes).

The Government's argument that the scienter requirement in subsection 1030(a)(5)(A) applies only to the "accesses" phrase is premised primarily upon the difference between subsection (a)(5)(A) and its predecessor in the 1984 statute. The decision to state the scienter requirement only once in subsection (a)(5)(A), along with the decision to change it from "knowingly" to "intentionally," are claimed to evince a clear intent upon the part of Congress to apply the scienter requirement only to the "accesses" phrase, though making that requirement more difficult to satisfy. This reading would carry out the Congressional objective of protecting the individual who "inadvertently 'stumble[s] into'

someone else's computer file." Senate Report at 6, U.S. Code Cong. & Admin. News at 2483.

The Government also suggests that the fact that other subsections of section 1030 continue to repeat the scienter requirement before both phrases of a subsection is evidence that Congress selectively decided within the various subsections of section 1030 where the scienter requirement was and was not intended to apply. Morris responds with a plausible explanation as to why certain other provisions of section 1030 retain dual intent language. Those subsections use two different *mens rea* standards; therefore it is necessary to refer to the scienter requirement twice in the subsection. For example, subsection 1030(a)(1) covers anyone who

> (1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data . . . with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

Since Congress sought in subsection (a)(1) to have the "knowingly" standard govern the "accesses" phrase and the "with intent" standard govern the "results" phrase, it was necessary to state the scienter requirement at the beginning of both phrases. By contrast, Morris argues, where Congress stated the scienter requirement only once, at the beginning of the "accesses" phrase, it

was intended to cover both the "accesses" phrase and the phrase that followed it.

There is a problem, however, with applying Morris's explanation to subsection 1030(a)(5)(A). As noted earlier, the predecessor of subsection (a)(5)(A) explicitly placed the same mental state requirement before both the "accesses" phrase and the "damages" phrase. In relevant part, that predecessor in the 1984 statute covered anyone who "*knowingly accesses* a computer without authorization, . . . *and* by means of such conduct *knowingly uses*, modifies, destroys, or discloses information in, or prevents authorized use of, such computer. . . ." 18 U.S.C. § 1030(a)(3) (Supp. II 1984) (emphasis added). This earlier provision demonstrates that Congress has on occasion chosen to repeat the same scienter standard in the "accesses" phrase and the subsequent phrase of a subsection of the Computer Fraud Statute. More pertinently, it shows that the 1986 amendments adding subsection (a)(5)(A) placed the scienter requirement adjacent only to the "accesses" phrase in contrast to a predecessor provision that had placed the same standard before both that phrase and the subsequent phrase.

Despite some isolated language in the legislative history that arguably suggests a scienter component for the "damages" phrase of subsection 1030(a)(5)(A), the wording, structure, and purpose of the subsection, examined in comparison with its departure from the format of its predecessor provision persuade us that the "intentionally" standard applies only to the "accesses" phrase of subsection 1030(a)(5)(A), and not to its "damages" phrase.

II. The unauthorized access requirement in subsection 1030(a)(5)(A)

Subsection 1030(a)(5)(A) penalizes the conduct of an individual who "intentionally accesses a Federal interest computer without authorization." Morris contends that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes. Morris argues that there was insufficient evidence to convict him of "unauthorized access," and that even if the evidence sufficed, he was entitled to have the jury instructed on his "theory of defense."

We assess the sufficiency of the evidence under the traditional standard. Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail (SEND MAIL), and to find out certain information about the users of other computers (finger demon). The question is whether Morris's transmission of his worm constituted exceeding authorized access or accessing without authorization.

The Senate Report stated that subsection 1030(a)(5)(A), like the new subsection 1030(a)(3), would "be aimed at 'outsiders,' *i.e.*, those lacking authorization to access any Federal interest computer." Senate Report at 10, U.S. Code Cong. & Admin. News at 2488. But the Report also stated, in concluding its discussion on the scope of subsection 1030(a)(3), that it applies "where the offender is completely outside the Government, . . . *or where the offender's act of trespass is interdepartmental in nature.*" *Id.* at 8, U.S. Code Cong. & Admin. News at 2486 (emphasis added).

Morris relies on the first quoted portion to argue that his actions can be characterized only as exceeding authorized access, since he had authorized access to a federal interest computer. However, the second quoted portion reveals that Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers. *See, e.g., id.* (stating that a Labor Department employee who uses Labor's computers to access without authorization an FBI computer can be criminally prosecuted).

The evidence permitted the jury to conclude that Morris's use of the SEND MAIL and finger demon features constituted access without authorization. While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris's conduct here falls well into the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

Moreover, the jury verdict need not be upheld solely on Morris's use of SEND MAIL and finger demon. As the District Court noted, in denying Morris' motion for acquittal,

> Although the evidence may have shown that defendant's initial insertion of the worm simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program. Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. Accordingly, the evidence did support the jury's conclusion that defendant accessed without authority as opposed to merely exceeding the scope of his authority.

In light of the reasonable conclusions that the jury could draw from Morris's use of SEND MAIL and finger demon, and from his use of the trusted hosts feature and password guessing, his challenge to the sufficiency of the evidence fails.

Morris endeavors to bolster his sufficiency argument by contending that his conduct was not punishable under (a)(5) but was punishable under (a)(3). That concession belies the validity of his claim that he only exceeded authorization rather than made unauthorized access. Neither (a)(3) nor (a)(5) punishes conduct that exceeds authorization. Both punish a person who "accesses" "without authorization" certain computers. Subsection (a)(3) covers the computers of a department or agency of the United States; subsection (a)(5) more broadly covers any federal interest computers, defined to include, among other computers, those used exclusively by the United States, 18 U.S.C. § 1030(e)(2)(A), and adds the element of causing damage or loss of use of a value of $1,000 or more. If Morris violated (a)(3),

as he concedes, then his conduct in inserting the worm into the INTERNET must have constituted "unauthorized access" under (a)(5) to the computers of the federal departments the worm reached, for example, those of NASA and military bases.

To extricate himself from the consequence of conceding that he made "unauthorized access" within the meaning of (a)(3), Morris subtly shifts his argument and contends that he is not within the reach of (a)(5) at all. He argues that (a)(5) covers only those who, unlike himself, lack access to *any* federal interest computer. It is true that a primary concern of Congress in drafting (a)(5) was to reach those unauthorized to access any federal interest computer. The Senate Report stated, "[T]his subsection [(a)(5)] will be aimed at 'outsiders,' *i.e.*, those lacking authorization to access any Federal interest computer." Senate Report at 10, U.S. Code Cong. & Admin. News at 2488. But the fact that the subsection is "aimed" at such "outsiders" does not mean that its coverage is limited to them. Congress understandably thought that the group most likely to damage federal interest computers would be those who lack authorization to use any of them. But it surely did not mean to insulate from liability the person authorized to use computers at the State Department who causes damage to computers at the Defense Department. Congress created the misdemeanor offense of (a)(3) to punish intentional trespasses into computers for which one lacks authorized access; it added the felony offense of (a)(5) to punish such a trespasser who also causes damage or loss in excess of $1,000, not only to computers of the United States but to any computer within the definition of federal interest computers. With both provisions, Congress was punishing those, like Morris, who, with

access to some computers that enable them to communicate on a network linking other computers, gain access to other computers to which they lack authorization and either trespass, in violation of (a)(3), or cause damage or loss of $1,000 or more, in violation of (a)(5).

Morris also contends that the District Court should have instructed the jury on his theory that he was only exceeding authorized access. The District Court decided that it was unnecessary to provide the jury with a definition of "authorization." We agree. Since the word is of common usage, without any technical or ambiguous meaning, the Court was not obliged to instruct the jury on its meaning. *See, e.g., United States v. Chenault*, 844 F.2d 1124, 1131 (5th Cir. 1988) ("A trial court need not define specific statutory terms unless they are outside the common understanding of a juror or are so technical or specific as to require a definition.").

An instruction on "exceeding authorized access" would have risked misleading the jury into thinking that Morris could not be convicted if some of his conduct could be viewed as falling within this description. Yet, even if that phrase might have applied to some of his conduct, he could nonetheless be found liable for doing what the statute prohibited, gaining access where he was unauthorized and causing loss.

Additionally, the District Court properly refused to charge the jury with Morris's proposed jury instruction on access without authorization. That instruction stated, "To establish the element of lack of authorization, the government must prove beyond a reasonable doubt that Mr. Morris was an 'outsider,' that is, that he was not authorized to access any Federal interest computer in any manner." As the analysis of the legislative history

reveals, Congress did not intend an individual's authorized access to one federal interest computer to protect him from prosecution, no matter what other federal interest computers he accesses.

Conclusion

For the foregoing reasons, the judgment of the District Court is affirmed.

APPENDIX B

JUDGMENT INCLUDING SENTENCE UNDER
THE SENTENCING REFORM ACT
Case No. 89-CR-139

UNITED STATES DISTRICT COURT
Northern District of New York

UNITED STATES OF AMERICA

V.

ROBERT TAPPAN MORRIS, Defendant

Thomas A. Guidoboni, Esq.
Defendant's Attorney

Filed in the US DISTRICT COURT N.D. OF N.Y.
May 16, 1990

The Defendant was found guilty on Count 1 of the Indictment after a plea of not guilty.

Accordingly the defendant is adjudged guilty of such count(s) which involve the following offenses:

Count 1, 18 USC, Sec. 1030 (a)(5), Intentional access of Federal interest computers without authorization thereby preventing authorized access and causing a loss in excess of $1,000.00.

The defendant is sentenced as provided in pages 2 through 7 of this Judgment. The sentence is imposed pursuant to the

Sentencing Reform Act of 1984,

The mandatory special assessment is included in the portion of this judgment that imposes a fine.

It is further ordered that the defendant shall notify the United States Attorney for this district within 30 days of any change of residence or mailing address until all fines, restitution, costs, and special assessments imposed by this Judgment are fully paid.

Defendant's Soc. Sec. Number: 572-82-5938

Defendant's mailing address:
6 Holly Avenue
Cambridge, MA 02138

Defendant's residence address: same as above.

Date of Imposition of Sentence, May 4th, 1990

Howard G. Munson, Judicial Official

May 16, 1990

PROBATION

The defendant is hereby placed on probation for a term of three years.

While on probation, the defendant shall not commit another Federal, state, or local crime and shall comply with the standard conditions that have been adopted by this court (set forth on the following page). If this Judgment imposes a fine or a restitution obligation, it shall be a condition of probation that the defendant pay any such fine or restitution. The defendant shall comply with the following additional conditions:

1. Robert Tappan Morris shall perform 400 hours of com-

munity service in a manner determined by the Probation Office and approved by the Court.

STANDARD CONDITIONS OF SUPERVISION

While the defendant is on probation or supervised release pursuant to this Judgment:

1) The defendant shall not commit another Federal, state or local crime;

2) the defendant shall not leave the judicial district without the permission of the court or probation officer;

3) the defendant shall report to the probation officer as directed by the court or probation officer and shall submit a truthful and complete written report within the first five days of each month;

4) the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;

5) the defendant shall support his or her dependents and meet other family responsibilities;

6) the defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training or other acceptable reasons;

7) the defendant shall notify the probation officer within seventy-two hours of any change in residence or employment;

8) the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any narcotic or other controlled substance, or any paraphernalia related to such substances, except as prescribed by a physician;

9) the defendant shall not frequent places where controlled subtances are illegally sold, used, distributed, or adminstered;

10) the defendant shall not associate with any persons engaged in crimnal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer;

11) the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view by the probation officer;

12) the defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;

13) the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcment agency without permission of the court;

14) as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

These conditions are in addition to any other conditions imposed by this Judgment.

FINE WITH SPECIAL ASSESSMENT

The defendant shall pay to the United States the sum of $10,050., consisting of a fine of $10,000. and a special assessment of $50.

These amounts are the totals of the fines and assessments imposed on individual counts, as follows:

On Count 1 of the Indictment. The Special Assessment of $50. is due immediately and should be made payable to Clerk, USDC/NDNY.

This sum shall be paid as follows:

The fine of $10,000. must be paid during the first year of probation in amounts determined by the Probation Officer.

RESTITUTION, FORFEITURE, OR OTHER PROVISIONS OF THE JUDGMENT

It is further Ordered that Robert Tappan Morris pay for the cost of his supervision at a rate of $91.00 per month as directed by the Probation Office.

The Court has determined that formulating an Order of restitution would unduly complicate and prolong the sentencing process.

See addendum

ADDENDUM

The Probation Officer, using the guideline for 2Fl.1., as reflected in Appendix A of the Statutory Index of the US Sentencing Commission Guideline Manual, has found the base Offense Level to be 6. The Total Offense Level to be 14 and the Criminal History Category to be 1. Guideline Range to be 15 to 21 months. The Probation Officer, however, finds that a new sentencing statute permits the court to depart from the Guideline-specified sentence when it finds, "an aggravating or mitigating of a kind or to a degree not adequately taken into consideration by the Sentencing Commission," and recommends a downward departure.

The Court agrees with the Probation Officer that there is no applicable guideline at this time for this specific offense. The court will not accept the scoring of this offense by the Probation Officer under the guideline for "Fraud and Deceit," but will depart for the following reasons:

1. It is the conclusion of this court that the characteristics of this case were not the type of case, "heartland case," used by the Sentencing Commission in placing 18 USC 1035(a)(5) under the Fraud and Deceit Guideline and that the Commission did not adequately take into consideration the specific characteristics of this type of case in considering alternative guidelines.

2. Although in and of itself, this offense is an extremely serious offense, by placing it in the Fraud and Deceit guideline in this specific case the total dollar lost overstates the seriousness of the offense.

3. Because of the lack of similar prosecutions of this type available to the Sentencing Commission, there was not sufficient information to establish any other

appropriate guideline when 18 USC 1035(a)(5) was placed in the Fraud and Deceit Category.

4. Under these circumstances, section 2X5.1 of the Sentencing Guidelines provides that "if there is not a sufficiently analogous guideline, the provisions of 18 USC 3553(b) shall control." Section 3553(b) in turn provides that "in the absence of an applicable sentencing guideline, the court shall impose an appropriate sentence, having due regard for the purpose set forth in subsection (a)(2). In the absence of an applicable sentencing guideline in the case of an offense other than a petty offense, the court shall also have due regard for the relationship of the sentence imposed to sentences prescribed by the guidelines applicable to similar offenses and offenders, and to the applicable policy statements of the Sentencing Commission."

dated: May 16, 1990

Hon. Howard G. Munson
US District Judge
Northern District of New York

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

89-CR-139

UNITED STATES OF AMERICA,

vs.

ROBERT TAPPAN MORRIS,
Defendant.

TRANSCRIPT OF PROCEEDINGS in the above-entitled matter, Motion Decision, held in United States District Court, Northern District of New York, James T. Foley U.S. Courthouse, Albany, New York, on Tuesday, February 27, 1990, before the Hon. Howard G. Munson, U.S. District Judge, presiding.

APPEARANCES:

UNITED STATES DEPARTMENT OF JUSTICE,
Fraud Section, Criminal Division
1400 New York Avenue, N.W., Room 2416
Washington, DC 20005
BY: MARK D. RASCH, ESQ.

BONNER & O'CONNELL, ESQS.
900 Seventeenth Street, N.W.
Washington, D.C. 20006
Attorneys for Defendant Morris
BY: THOMAS A. GUIDOBONI, ESQ.

THE COURT: Well, gentlemen, I'm going to decide this case right now. I'm probably going to say more than is necessary, but I think perhaps I should give a little background on this case. As we're all aware, on January 22nd, 1990, the

defendant Robert Tappan Morris was found guilty of violating Section 1030(a)(5) of the Computer Fraud and Abuse Act of 1986. The defendant now moves for a judgment of acquittal pursuant to Federal Rule 29(c) or alternatively for a new trial under Rule 33.

In support of his motion for judgment of acquittal, the defendant contends that the evidence adduced at trial was insufficient to permit a rational juror to conclude that each element of the offense charged was established beyond a reasonable doubt. More specifically, defendant argues that the Government failed to carry its burden in demonstrating that he, number 1, accessed without authority, and number 2, that he acted with the necessary intent as required by the statute.

Insofar as the defendant is moving in the alternative for a new trial, the defendant contends that the interests of justice and fairness demand a new trial because this Court's jury instruction was inadequate, the prosecutor's closing argument was prejudicial, and otherwise irrelevant and prejudicial evidence was offered during the trial. I will address each of those arguments that were raised by the defendant.

Let me first talk about judgment of acquittal. But before discussing the substance of defendant's arguments for judgment of acquittal, let me briefly summarize the principles that guide the Court in deciding such a motion. I think we are all in agreement with it, but I'll still do it. In the *United States versus Chang An-Lo*, 851 F.2d 547, a 1988 Second Circuit case, the court said the defendant bears a very heavy burden in challenging the sufficiency of the evidence. The test is whether the jury drawing reasonable inferences from the evidence may fairly and logically have concluded that the defendant was guilty beyond a reasonable doubt. In making such a determination, the evidence is viewed in the light most favorable to the Government and all permissible inferences are

construed in its favor. If any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt, the conviction must be sustained.

As the Second Circuit noted in *United States versus Mariani*, 725 F.2d 862, a 1984 Second Circuit case, these strict rules are necessary to avoid judicial usurpation of the jury function. The Court should not substitute its own determination of the credibility of witnesses, the weight of the evidence and the reasonable inferences to be drawn for that of the jury. Although the defendant's arguments in support of its motion for judgment of acquittal are framed in terms of a challenge to the sufficiency of the evidence, I think that the defendant is in reality revisiting legal arguments which this Court has previously rejected in denying his pretrial motion to dismiss the indictment and in his previous motions for judgment of acquittal at the end of the Government's and his case.

Given the lack of prior judicial interpretation of the statute under which the defendant was charged and subsequently convicted, this Court has been called upon to undertake its own independent analysis of the statute's essential elements and intended application as well as its constitutionality as applied in this case. In doing so, this Court has examined the text of the statute, prior versions of the statute, and the available legislative history. The Court believes that its previous rulings are supported by the language of the statute consistent with the congressional intent and in conformity with constitutional requirements. The Court at this time has not been presented with any compelling arguments for reconsidering its prior interpretation of the necessary elements of the statute, and accordingly will not do so now.

Therefore, I will proceed to examine the sufficiency of the evidence in the light of my prior legal conclusions with respect

to the elements of Section 1030(a)(5). When so viewed, the Court holds that there was, in fact, sufficient evidence as to each and every element of the crime charged to support the jury's verdict.

First, as to the requisite intent under the statute, this Court ruled on November 3rd, 1989, in denying defendant's motion to dismiss the indictment that the language and grammatical structure of the statute indicates to the Court that the requirement of intent is only applicable to the conduct of accessing and is unrelated to the resulting damage. Thus, this Court rejected at that time as it does now the argument that the intent to prevent authorized use and thereby cause loss was an element of the offense. Given this construction, the defendant's argument that there was insufficient evidence to prove that the defendant acted with the requisite intent must fail because, in fact, there was ample evidence for a rational juror to find beyond a reasonable doubt that the defendant intentionally accessed computers without authorization. Indeed, it's my recollection that the defendant's own testimony was sufficient to establish that fact.

Furthermore, given this Court's interpretation of the requisite intent, defendant's related argument that there was insufficient evidence to prove beyond a reasonable doubt that defendant acted willfully must also fail. Defendant argues in this regard that, since the indictment charging the defendant with violating Section 1030(a)(5) stated among other things that the defendant caused to be accessed federal interest computers, the Government was also required to establish as required by 18 U.S.C. 2(b) that defendant willfully caused the commission of a forbidden act. Notwithstanding the defendant's contention to the contrary, there was sufficient evidence to support the jury's verdict that defendant willfully caused the commission of the act proscribed by Section 1030(a)(5), namely accessing federal interest computers without authorization.

Defendant also challenges the insufficiency of the evidence with respect to the element accessing without authority. Defendant contends that the evidence presented during the trial indicate or indicated that the defendant had express authority to access several federal interest computers; namely computers at Cornell, at Harvard University and at the University of California at Berkley, and implicit authorization to access other computers by means of electronic mail and the Finger and FTP programs. Defendant asserts that this evidence in itself is sufficient to acquit him because at most the evidence indicated that he exceeded his authority which is not subject to criminal prosecution under Section 1030(a)(5). In this regard defendant directs the Court's attention to sections of the legislative history which in defendant's opinion confirm the fact that Congress would consider the conduct which he engaged in to be that of an insider and therefore beyond the scope of criminal sanction of the computer fraud statute.

Viewing the evidence in the light most favorable to the Government, as the Court must, the Court concludes that there was sufficient evidence to permit a rational juror to conclude the defendant did, in fact, access without authority as opposed to simply exceeding the scope of his authority. Contrary to the defendant's argument, merely because he had authority to access some computers does not preclude the jury from reasonably concluding that the defendant did not have authority to access other computers.

Although the evidence may have shown that defendant's initial insertion of the worm simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program. Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. Accordingly, the

evidence did support the jury's conclusion that defendant accessed without authority as opposed to merely exceeding the scope of his authority.

Furthermore, the Court rejects defendant's argument that the trial evidence merely indicated that he engaged in conduct which should be characterized as that of an insider, as that term is used in the legislative history of the Act. The defendant is correct in concluding that the drafters of Section 1030(a)(5) only intended outsiders, that is those lacking access to any federal interest computer, to be subject to criminal prosecution. Nonetheless, it is clear from the committee report that an individual who has authority to access one computer and intentionally uses that authority to obtain access to another computer to which he or she is unauthorized to access, such as the defendant in this case, would be deemed an outsider and therefore properly subject to criminal prosecution. As such, the defendant — the Court denies the defendant's motion for judgment of acquittal.

Now, the defendant alternatively contends that the interests of justice require a new trial under Rule 33. Two of defendant's principle arguments in this regard I think can be quickly disposed of. First the defendant asserts that the court's jury instruction was defective as to the elements of intent, without authorization, willfulness and loss. After reviewing the jury charge on these elements, I find that the instructions were appropriate and that the defendant was not substantially prejudiced by the charge that was provided. Accordingly, I do not believe that the interests of justice necessitate a new trial on the grounds of claimed inadequate jury instructions.

Second, the defendant claims that irrelevant and prejudicial evidence regarding the loss sustained as a result of defendant's conduct also requires a new trial. I reject this contention in addition. A rational juror could have found that the defendant caused a loss in excess of $1,000, and they could have found

that beyond a reasonable doubt. Any prejudice which the defendant may have suffered as a result of the admission of irrelevant evidence in this regard does not rise to the level of demanding a new trial.

Defendant's final argument in support of a new trial, however, I think demands a little more scrutiny. Defendant argues that the Goverment's closing argument was improper and highly prejudicial in that, by comparing the defendant's acts to that of a terrorist or a drunk driver, the Government appealed to issues irrelevant to the case and designed to inflame the jury's emotion and prejudice, and he does so, in addition, in the light of the death of 23 Syracuse University students in December of 1988.

Although the Court at the time the statement was made sustained the defendant's objection, this Court does not believe that the prosecution's statement in itself mandates a new trial. The Second Circuit has held in several cases that, before a court may grant a new trial on the basis of a prosecutor's misconduct, the Court must ascertain whether the prosecutor's misconduct was substantial or caused substantial prejudice to the defendants thereby depriving them of their rights to a fair trial. I refer you to the *United States versus Biasucci*, that's 786 F.2d 504, certiorari denied at 479 U.S. 827; *United States versus Pinto*, 850 F.2d 927, a 1988 Second Circuit case; and the *United States versus Modica*, 663 F.2d 1173, 1981 Second Circuit case, and certiorari was also denied at 456 U.S. 989.

The Second Circuit has also noted that criminal convictions are not to be lightly overturned on the basis of a prosecutor's inappropriate comments standing alone in an otherwise fair proceeding. Therefore, in determining whether a new trial should be granted, the Court must assess the severity of the misconduct, the measures adopted to cure the misconduct and

the certainty of conviction absent the improper statement. In weighing these factors, this Court concludes that a new trial is not warranted.

First, although the Court did not provide a curative instruction, the Court did sustain the objection. Second, the objectionable comparison was merely one isolated event in the trial which in my opinion was otherwise free from appeals to prejudice and emotion. Finally, as discussed previously this morning, there was substantial evidence of defendant's guilt even without the objectionable comment. Accordingly, whatever prejudice the defendant may have suffered as a result of the Government's closing argument is not substantial enough to warrant a new trial.

On the basis of what I've just said, I'm going to set the sentencing date for Mr. Morris for Friday, the 4th of May at 2 o'clock in the afternoon, that's 1990, at 2 o'clock in the afternoon, at Syracuse, New York.

MR. GUIDOBONI: I'm sorry, at Syracuse?

THE COURT: Yes, at Syracuse. In sum, the defendant's motion for a judgment of acquittal and for a new trial is denied. This represents the final decision and order of this Court, and no written order shall issue. I would like to see both counsel if I may, Mr. Morris may come if he desires, but I'd like to see them in Judge Foley's chambers.

THE CLERK: Court stands in recess.

(Whereupon, the matter was concluded.)

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

89-CR-139

UNITED STATES OF AMERICA,

Plaintiff,

vs.

ROBERT TAPPAN MORRIS,
Defendant.

TRIAL, Proceedings held on January 18, 1990, at the United States Courthouse, Syracuse, New York, before the HONORABLE HOWARD G. MUNSON, United States District Court Judge, Northern District of New York.

APPEARANCES:

U.S. DEPARTMENT OF JUSTICE
For the United States
BY: MARK D. RASCH, Trial Attorney
and
ELLEN MELTZER, Trial Attorney

BONNOR & O'CONNELL
Attorneys for the Defendant
BY: THOMAS GUIDOBONI, ESQ., Of Counsel
and
DAVID O'BRIEN, ESQ., Of Counsel

HANCOCK & ESTABROOK
Local Counsel for the Defendant
BY: MARK J. SCHULTE, ESQ., Of Counsel

KENNETH H. CREWELL, JR.
Official U.S. Court Reporter
100 South Clinton Street
(315) 423-5530

THE COURT: I understand what you are saying, Mr. Guidoboni. No, given the standard that I must consider on a Rule 29 motion at this stage of the proceeding, your motion is denied and you have an exception.

* * *

MR. GUIDOBONI: Thank you, Your Honor.

MR. RASCH: Thank you, Your Honor.

COURT CLERK: Court stands adjourned.

THE COURT: You have an exception, of course, Mr. Guidoboni.

(WHEREUPON, COURT WAS ADJOURNED.)

(END OF PROCEEDINGS HELD ON JANUARY 18, 1990)

* * *

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

89-CR-139

UNITED STATES OF AMERICA,

Plaintiff,

vs.

ROBERT TAPPAN MORRIS,
Defendant.

TRIAL, Proceedings held on January 17, 1990, at the United States Courthouse, Syracuse, New York, before the HONORABLE HOWARD G. MUNSON, United States District Court Judge, Northern District of New York.

APPEARANCES:

U.S. DEPARTMENT OF JUSTICE
For the United States
BY: MARK D. RASCH, Trial Attorney
and
ELLEN MELTZER, Trial Attorney

BONNOR & O'CONNELL
Attorneys for the Defendant
BY: THOMAS GUIDOBONI, ESQ., Of Counsel
and
DAVID O'BRIEN, ESQ., Of Counsel

HANCOCK & ESTABROOK
Local Counsel for the Defendant
BY: MARK J. SCHULTE, ESQ., Of Counsel

KENNETH H. CREWELL, JR.
Official U.S. Court Reporter
100 South Clinton Street
(315) 423-5530

* * *

THE COURT: Well, part of the arguments that you have made, if not all of them, was made at the time that the motions were made on behalf of the Defendant in this case back I think last November.

At this time , I'm going to deny your motion, Mr. Guidoboni. You have an exception to that denial, and I deny it partially based upon the decision of the Court earlier with regard to the arguments that you made at that time, but also based upon the proof that's been introduced in this case and the standard that the Court must comply with at this stage of the case when it considers a Rule 29 motion for judgment of acquittal.

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

89-CR-139

UNITED STATES OF AMERICA,

Plaintiff,

vs.

ROBERT TAPPAN MORRIS,
Defendant.

APPEARANCES:

FREDERICK J. SCULLIN, JR.
United States Attorney
Northern District of New York
100 S. Clinton St.
Syracuse, New York 13260

MARK D. RASCH, ESQ.
U.S. Department of Justice

ELLEN R. MELTZER, ESQ.
U.S. Department of Justice

ANDREW T. BAXTER, ESQ.
Assistant United States Attorney

HANCOCK & ESTABROOK
Local counsel for Defendant
MONY Tower I
P.O. Box 4976
Syracuse, New York 13221

MARK J. SCHULTE, ESQ.

BONNOR & O'CONNELL
Attorneys for the Defendant
Suite 1000
900 17th St. N.W.
Washington, D.C. 20006

THOMAS GUIDOBONI, ESQ.

HOWARD G. MUNSON, J.

MEMORANDUM-DECISION & ORDER

The United States has moved to withdraw a portion of the indictment charging defendant with violating 18 U.S.C.

§ 1030(a)(5). Specifically, the United States seeks to withdraw from the indictment any reference to "Air Force Logistics Command, Wright Patterson Air Force Base in Dayton, Ohio." The government seeks this withdrawal because it no longer intends to offer any evidence at trial to prove that the Wright Patterson computer was one of the Federal interest computers intentionally accessed by defendant.

The government has not cited, and this court has not found, any cases in which the government has moved prior to trial to withdraw a portion of the indictment. However, as defendant correctly recognizes, at least since the Supreme Court's decision in *United States v. Miller*, 471 U.S. 130 (1985), it is clear that during the course of a trial a court may "drop from an indictment those allegations that are unnecessary to an offense that is clearly contained within it," *id.*, at 144, and may withdraw from the jury's consideration portions of the indictment that are not supported by the evidence adduced at trial without violating a defendant's Fifth Amendment right to a grand jury. *See also Salinger v. United States*, 272 U.S. 542 (1926); *United States v. Anguilo*, 847 F.2d 956, 964 (1st Cir.), *cert. denied*, 109 S. Ct. 138 (1988). If the criminal charges against the defendant are not broadened, such withdrawal does not constitute an unconstitutional amendment of the indictment. *See Russell v. United States*, 369 U.S. 749 (1962); *Stirone v. United States*, 361 U.S. 212 (1960). Therefore, if the government, instead of making the present motion, proceeded to trial on the existing indictment but failed to introduce any evidence that defendant accessed the computer at the Wright Patterson Air Force Base the court could properly withdraw this allegation in the indictment from the jury's consideration without infringing upon any constitutional guarantees of the defendant. The court does not discern any legitimate reason for reaching a different conclusion when prior to trial the government seeks to withdraw an allegation

in the indictment for which it does not intend to offer any proof.[1] Accordingly, the court does not find persuasive defendant's argument that resubmittion to the grand jury is necessary because "it cannot be said that an indictment would have been returned in absence of evidence of the value of the loss allegedly suffered by 'the Air Force Logistics Command, Wright Patterson Air Force Base in Dayton, Ohio.' " So long as the narrowed indictment alleges the essential elements of the charged offense, sufficiently informs the defendant of the charges which he must defend, enables him to plead it to bar future prosecutions for the same offense, and does not broaden the charges against the defendant there is no Fifth Amendment difficulty. *See United States v. Miller*, 471 U.S. at 135; *United States v. Anguillo*, 847 F.2d at 964.

The proposed revised indictment satisfies each of these requirements. First, it continues to allege the necessary elements to charge an offense under 18 U.S.C § 1030(a)(5), namely, intentionally accessing a federal interest computer without authorization, preventing authorized use of one or more of such computers, and causing a loss to one or more others of a value aggregating at least $1000 during any one year period. Second, the proposed withdrawal of any reference to Wright Patterson Air Force Base does not alter this court's prior ruling that the indictment adequately informs the defendant of the crime which he is charged, thus permitting him to prepare his defense and to protect himself against future prosecutions for the same charge. In addition, since the proposed indictment does not broaden the charge against the defendant, the court rejects defendant's contention that the

[1]Indeed, a pretrial motion to withdraw a portion of an indictment is arguably more favorable to a criminal defendant that if the withdrawal occurs during trial. A jury is likely to infer from the court's failure to withdraw other portions of the indictment that defendant committed the remaining acts specified in the indictment.

proposed withdrawal will allow the government to prosecute defendant for a crime different than originally charged by the grand jury. Accordingly, the United State's motion is granted.

It is so ordered.

Dated: January 3, 1990
Syracuse, New York.

HOWARD G. MUNSON
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

No. 89-CR-139

UNITED STATES OF AMERICA,
v.

ROBERT TAPPAN MORRIS

TRANSCRIPT OF DECISION on Defendant's Motions to Dismiss, rendered by the Honorable Howard G. Munson, Northern District of New York, United States Courthouse, Syracuse, New York, in proceedings held on November 3, 1989.

A P P E A R A N C E S

For the Plaintiff:
HON. F.J. SCULLIN, JR.
James M. Hanley Federal Building
Syracuse, New York 13206
BY ANDREW T. BAXTER, AUSA

For the Defendant:
BONNER & O'CONNELL
Attorneys at Law
900 Seventeenth Street, N.W.
Washington, D.C. 20006
BY: THOMAS A. GUIDOBONI, ESQ.

and

HANCOCK & ESTABROOK
Attorneys at Law
MONY Tower I
Syracuse, New York 13221-4976
BY MARK J. SCHULTE, ESQ.

THE CLERK: United States of America versus Robert Tappan Morris, 89-CR-139. Gentlemen, please come forward and note your appearance for the record.

MR. BAXTER: Good afternoon. Andrew Baxter for the United States.

MR. GUIDOBONI: Thomas Guidoboni, Bonner & O'Connell, for Defendant Robert Tappan Morris.

THE COURT: Well, is there anything else anyone would like to add to what they said last time you were here?

MR. BAXTER: Nothing for the Government, your Honor.

MR. GUIDOBONI: No, your Honor, we'll submit on the arguments.

THE COURT: All right, then, let me start with the defendant as to the arguments that they submitted in support of their motion to dismiss the indictment. First of all, the defendant contends that the Government's alleged violation of its own internal regulations and a breach of the cooperation agreement with the defendant warrants dismissal of this indictment for prosecutorial misconduct. Secondly, the defendant challenges the legal sufficiency of the indictment in that it fails to allege that the defendant acted with the requisite intent for the crime charged, is vague and overly generalized and fails to show jurisdiction in this Court. And third and finally, the defendant seeks dismissal of the indictment because, in the defendant's view, the statute upon which the indictment is based is unconstitutionally vague. I'll address each one of those arguments.

First of all, with regard to prosecutorial misconduct, for the purposes of deciding Defendant's motion to dismiss on the basis of prosecutorial misconduct only, this Court will assume that the indictment is in all other aspects legally sufficient. In

this Circuit, as in others, dismissal of an indictment for prosecutorial misconduct is the rare exception rather than the general rule. It's well established that dismissal of an indictment pursuant to the federal court's supervisory power over the criminal justice system is reserved only for the most extreme of circumstances. In *United States v. Fields*, 592 F.2d, a 1978 Second Circuit case, wherein certiorari was denied, the Second Circuit addressed the standard by which a motion to dismiss for prosecutorial misconduct must be assessed. In discussing the purposes of such a dismissal, the Court noted that "the extreme sanction of dismissal of an indictment is justified in order to achieve one or both of two objectives. First,to eliminate prejudice to a defendant in a criminal prosecution; and second, to 'help translate the assurances of United States Attorneys into consistent performances by their assistants.' " The Court further oberves that "it is only in the rare case where it is impossible to restore a criminal defendant to a position that he would have occupied a vis-a-vis prosecutor, that the indictment may be dismissed . . . Proper regard for the public interest in the prosecution of crimes counsels restraint in dismissing an indictment for deterrence purposes, unless the course of official misconduct is demonstrated and is a long-standing one. We have approved this extreme sanction only when the pattern is widespread and continuous," the Court said. And that, again, is *United State v. Fields*, 592 F.2d.

In the present case, the Court need not decide whether the Government's pre-indictment public disclosures actually violated internal Justice Department regulations or breached the cooperation agreement with the defendant to rule upon Defendant's motion to dismiss on prosecutorial misconduct for, even assuming such a violation and breach, the defendant has not, in this Court's opinion, articulated any concrete prejudice that he has suffered as a result of these disclosures.

The newspaper articles submitted by Defendant merely disclose that the defendant had, in fact, made several statements under a limited grant of immunity and that the Government was considering whether to permit defendant to plead to a misdemeanor. The substance of any statements made by the defendant and any plea negotiations was not revealed. In the absence of specific evidence of actual prejudice, and given the Second Circuit's pronouncement that dismissal of an indictment for prosecutorial misconduct is a rare and extreme sanction, the Court will not presume prejudice before the grand jury from these disclosures. Moreover, the defendant's argument regarding prejudice to potential trial jurors is premature and, as the Government correctly argues, it is more appropriately dealt with in a jury selection process.

In addition, the Court does not believe that the Government's conduct was especially egregious so as to necessitate dismissal. In hindsight, the "leak" by the Justice Department attorney may have been imprudent and perhaps violated Justice Department regulations. However, as the standard for dismissal expressed in the *Fields* case, the Court does not believe that this extreme sanction is warranted on the facts presented. Accordingly, the defendant's motion to dismiss this indictment for prosecutorial misconduct is denied.

Now, as an alternative remedy for the Government's alleged breach of the cooperation agreement, the defendant seeks an order preventing the Government from derivatively using defendant's statement. The only explicit agreement made by the Government with regard to public disclosures was the United States Attorney's representation that it was not his intention to release a transcript of defendant's statement to the public. Since no such transcript was ever released, the Government did not breach its expressed promise. Moreover, even assuming that an implicit part of the cooperation agree-

ment was the Government's promise not to violate Justice Department regulations regarding public disclosure, as a defense claimed, the Court declines to grant defendant's motion for alternative relief, given the absence of actual prejudice to the defendant.

Let me talk about the arguments with regard to legal sufficiency of the indictment. As I said earlier, the defendant has moved to dismiss based upon his contention that the indictment is insufficient as a matter of law. Rule 7(c)(1) of the Federal Rules of Criminal Procedure provides that an "indictment shall be a plain, concise and definite written statement of the essential facts constituting the offense charged . . . It need not contain . . . any other matter not necessary to such statement." The Second Circuit has noted that the purpose of this rule is to promote simplicity in procedure and to avoid unnecessarily verbose indictments. And they said that in *United States v. Carrier,* 672 F.2d 300. Certiorari was also denied in that. They have said it in other cases, also. An indictment is sufficient as a matter of law "if it contains the elements of the offense charged and fairly informs a defendant of the charges against which he must defend and enables him to plead an acquittal or in bar for the future prosecutions for the same offense." It's from *United States v. Chestnut,* 533 F.2d 40.

Moreover, indictments are routinely upheld in this Circuit "if they do little more than track the language of the statute and state the time and place of the offense in approximate terms." And it's in *United States v. Beech-Nut Nutrition Corp.,* 659 F. Supp. 1487 (citing *U.S. v. Salazar*). And there are several other cases in the Second Circuit, for example *United States v. Bagaric,* 706 F.2d 42. The defendant does not contend that the indictment fails to track the statutory language. Rather, the defendant argues that the wording of the statute

is ambiguous with respect to the necessary intent required to charge the offense under Section 1030(a)(5). Defendant contends that the legislative history of the statute supports his position that Congress intended that an offense was committed under this statute only where the accused intentionally accesses a Federal interest computer and intentionally "alters, damages or destroys information . . . or prevents authorized use . . . and thereby causes loss . . . . Defendant argues that since the indictment only charges him with intentionally accessing a Federal interest computer and fails to allege that the defendant intentionally prevented authorized use and thereby caused loss, the indictment is legally insufficient.

Both the defendant and the Government cite exhaustively to the legislative history of the Computer Fraud and Abuse Act of 1986. They do that in support of their respective interpretation of Section 1030(a)(5). It is a fundamental principle of statutory construction, however, that "the starting point for interpreting a statute is the language of the statute itself." The Supreme Court of the United States said that in *Consumer Products Safety Commission v. G.T.E. Sylvania, Inc.*, 447 U.S. 10. Moreover, where the statute language is clear and unambiguous, judicial inquiry into the meaning of that statute is at an end. That's in *United States v. Payden*, 759 F.2d 202, a Second Circuit case in 1985. The Court is not convinced that Section 1030(a)(5) contains the latent ambiguity that the defendant suggests. The language and grammatical structure of the statute indicates to the Court that the requirement of intent is only applicable to the conduct of the "accessing" and is unrelated to the resulting damage. The defendant's proposed construction of the statute would not clarify an ambiguous statute; but rather, in my opinion, alter its clear meaning.

Indeed, it's interesting, although I think unnecessary, to note that the previous version of Section 1030(a)(5) was which was

codified at 18 U.S.C. 1030(a)(3) expressly contained the dual mental state requirement that the defendant would have this Court engraft upon the present statute. As originally enacted in 1984, the statute provided that "Whoever — knowingly accesses a computer without authorization . . . and by means of such conduct knowingly uses, modifies, destroys or discloses information in, or prevents authorized use of, such computer . . . shall be punished as provided in subsection (c) of this section." The present statute, as amended in 1986, not only changes the requisite mental state from knowingly to intentionally, but it also omits the necessity of demonstrating that the accused acted with any mental state with regard to the resulting damage. This obvious structural change in the statute is, to this Court, most persuasive evidence of Congress' intent, if one were needed. Moreover, a comparison of the present subsection (a)(1) with (a)(5) further supports the argument that Congress is well aware of how to draft a statute creating a mental state for both conduct and resulting damage or harm. Accordingly, the Court concludes that the indictment adequately alleges the necessary intent to charge offense under Section 1030(a)(5); and, therefore, Defendant's motion to dismiss on that basis is denied.

Defendant next contends that the indictment is indequate because it's vague and generalized. Specifically, defendant contends that the indictment does not adequately specify where the offense occurred, which computers were accessed, the nature of the loss, or the identity of the victims. The Court is not persuaded, however, that these omissions require dismissal. As noted earlier, the indictment tracks the statutory language and also states the approximate time and place of the offense charged. By so doing, the defendant was put on adequate note of the crime with which he is charged. The indictment is legally sufficient and will not be dismissed due to vagueness or generality. Of course, the defendant is not pre-

cluded from bringing on a motion before this Court for a bill of particulars or discovery if he believes that additional information is necessary to adequately prepare his defense.

Defendant's final argument with respect to the adequacy of his indictment is his contention that the indictment fails to show jurisdiction in the Court. Section 1030(a)(5) only proscribes intentional unauthorized access of Federal interest computers. As defined in the statute, Federal interest computer is "one of two or more computers used in committing the offense, not all of which are located in the same state." That's in 18 U.S.C. 1030(e)(2)(B). The indictment charges that "not all of the computers so accessed in the commission of the offense were located in the same state." The defendant believes that this disparity requires dismissal of the indictment; that is, the difference between the use of the word "used" and the use of the word "accessed." I think that this is an overly technical argument, and it really doesn't warrant much discussion. Jurisdiction is clearly established in the indictment by the phrase "defendant Robert Tappan Morris intentionally and without authorization accessed and caused to be accessed Federal interest computers." Moreover, because "use" and "access" are not defined in the statute, the Court will not impute to Congress an intention to use these terms other than in their ordinary meaning, and it seems to me that it would be difficult to conceive how one could "access" without simultaneously "using." Therefore, the Court concludes that the indictment does show jurisdiction in this Court and defendant's motion is denied.

Now, with regard to the constitutionality of Section 1030(a)(5), and this is the final argument, the defendant, in support of its motion to dismiss, asserts that this statute is unconstitutionally vague. To pass constitutional muster, a penal statute must "define the criminal offense with sufficient

definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." That is found in *Kolender v. Lawson*, 461 U.S. 352, a 1983 case. To succeed on a vagueness challenge, the moving party must "demonstrate that the law is impermissibly vague in all of its applications." *Village of Hoffman Estates v. The Flipside, Hoffman Estates, Inc.*, 455 U.S. 489.

Defendant contends that the absence of definitions of such key terms as "access" and "use" renders the statute unconstitutionally vague. The defendant then raises several hypothetical examples of situations that might conceivably be covered by the undefined language in the statute. Whether or not the statute would pose constitutional difficulties, the Court expresses no opinion. And I do that because it has been stated that since an individual" who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others." And in the Court's view, the defendant has failed to demonstrate that Section 1030(a)(5) is impermissibly vague as applied to him. An ordinary person, in reading the words of this statute, would know that whatever the outer limits of conduct proscribed by Seciton 1030(a)(5), the conduct that defendant is alleged to have engaged in, namely gaining entry into other computer systems without authorization and inserting a program designed to slow these computers to such a degree that its operators could not use them, would be prohibited by this statute. According, Section 1030(a)(5) is not unconstitutionally vague as applied to this defendant. Therefore defendant's motion to dismiss is denied.

In sum, defendant's motions to dismiss the indictment are denied in all respects.

APPENDIX C

18 U.S.C. § 1030 (1988)

Fraud and related activity in connection with computers

(a) Whoever—

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reasons to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is

used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;

(4) Knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

shall be punished as provided in subsection (c) of this section.

(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby —

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization. If—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is —

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for

another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section —

(1) the term ''computer'' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term ''federal interest computer'' means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

(4) the term "financial institution" means —

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and

(G) the Securities Investor Protection Corporation;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter; and

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

18 U.S.C. § 1030 (Supp. II 1984)

Fraud and related activity in connection with computers.

(a) Whoever —

(1) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), or contined in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(3) knowingly accesses a computer without authorization, or having accessed a computer with

authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;

shall be punished as provided in subsection (c) of this section. It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.

(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) The punishment for an offense under subsection (a) or (b)(1) of this section is —

(1)(A) a fine of not more than the greater of $10,000 or twice the value obtained by the offense or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1)

of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine of not more than the greater of $100,000 or twice the value obtained by the offense or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine of not more than the greater of $5,000 or twice the value obtained or loss created by the offense or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine of not more than the greater of $10,000 or twice the value obtained or loss created by the offense or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be execised in accord-

ance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section, the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.